REMARKS/ARGUMENTS

The applicant would like to acknowledge, with thanks, receipt of the Office Action mailed on May 18, 2007. This amendment is responsive to the May 18, 2007 Office Action. Reconsideration of the application as amended is requested for reasons that will be set forth below.

Claims 1, 9 and 17 have been amended. Claim 28 is new. The subject matter of claim 28 is not new matter as it is disclosed on page 4, lines 13-20 of the original specification.

CLAIM OBJECTIONS

Claims 1 and 9 were objected for lack of antecedent basis for certain claim elements. Accordingly, these claims have been amended to remedy the informalities and withdrawal of these objections is requested.

PRIOR ART REJECTIONS

Claims 1-24 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Funk (Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet Draft PPPEXT Working Group (Nov. 2002)(p. 1-40). For reasons that will now be se forth, claims 1-24, as they currently stand, are not anticipated by Funk.

Independent claims 1, 9 and 17, as currently amended, are directed to a method or system for providing a network access credential to a client. This enables a client to acquire a network access credential (e.g. a password or shared secret) in band (e.g. via a network device) as opposed to out of band (e.g. manually entered into the device). The network access credential can then be used by the client to access network services.

To obtain the network access credential, a secure tunnel is established between a first (e.g. server) and second (e.g. peer or client) parties. An encryption algorithm is employed to establish an encryption key for the tunnel. The client then authenticates with an authentication server of the secured tunnel. An authentication key is established during the authentication. The

first and second parties then verify they were the same parties that were involved in 1) establishing the tunnel and 2) performing the authentication by verifying that each party has the same keys (i.e. the same tunnel key and authentication key). For example (as recited in claims 25-27) each can party hash its first (e.g. tunnel) and second (e.g. authentication) key and then verifies the hash result obtained by the other party matches. If the hashes match, it is established that the first and second parties established both the tunnel key and authentication key.

Funk discloses establishing a secure tunnel, performing authentication within the tunnel. Funk discloses during phase 2, the TLS record layer is used to tunnel information between client and TTLS server to perform any number of functions such as "user authentication, negotiation of data communication security capabilities, key distribution, communication of accounting information, etc." (Funk § 6, page 12, 1st paragraph). Nowhere does Funk teach 1) that both parties verify their tunnel & authentication keys match the other party's nor providing a network access credential to the peer responsive to 1) successful establishment of the tunnel; 2) successful authentication; and 3) verifying keys each party acquired matching keys while establishing the tunnel and authenticating. Therefore, Funk does not disclose each and every element of independent claims 1, 9 and 17and thus does not anticipate claims 1, 9 and 17 as currently amended.

Claims 2-8, 10-16 and 18-28 depend from one of independent claims 1, 9 and 17 and therefore contain each and every element of one of claims 1, 9 and 17. Therefore, for reasons already set forth for claims 1, 9 and 17, claims 2-8, 10-16 and 18-28 are not anticipated by Funk.

Claims 25-27 stand rejected under 35 U.S.C. § 103(a) as being obvious in view of the combination of Funk and U.S. Patent Publication 2003/0226017 to Palekar et al. (*hereinafter* "Palekar"). For reasons that will now be set forth, claims 25-27 are not obvious in view of Funk and/or Palekar, when taken alone or in combination.

Claims 25-27 are dependent upon independent claims 1, 9 and 17 respectively and therefore contain each and every element of claims 1, 9 and 17 respectively. The aforementioned deficiency in Funk for claims 1, 9 and 17 is not remedied by any teaching of Palekar. In addition to the foregoing, claims 25-27 recite that the first device hashes the first party encryption key and first party authentication key to produce a first hash, the second device hashes the second party encryption key and the second party authentication key to produce a

second hash, and that the first and second hashes are compared to verify they are the same. As disclosed on page 11, lines 1-3 of the original disclosure, "the server and client must prove they ensured in both the tunnel establishment and MSCHAPv2 conversations by hashing the resulting keys of both conversations. If both parties prove they have computed the same hashing result, the server can then provision

The examiner relies on paragraphs [0008], [0044] and [0079] for disclosing these elements. Applicant respectfully disagrees.

Paragraph [0008] discloses protecting messages with the TLS protocol (also known as "a TLS tunnel") to protect the messages while en route from rogue interception. The tunnel can be used protect authentication messages. The protection can be realized by setting up the tunnel and postponing authentication until after the TLS tunnel has been created. Nowhere does paragraph [0008] disclose hashing the first device's first (e.g. tunnel) key, second (e.g. authentication) key to produce a first hash key, hashing the second device's first (e.g. tunnel) key, second (e.g. authentication) key to produce a second hash key, and comparing the first and second hash keys to verify they are the same. This enables both endpoints to verify that the other endpoint is the same device that 1) setup the tunnel; and 2) performed the authentication.

Paragraph [0044] discloses employing a password as a shared secret because both the server computing device and the user know the password. Most authentication mechanisms avoid sending the shared secret itself, and instead rely on security devices such as a one-way hash. For example, the server computing device can send a random value to the client, and the client can key-hash the value using the client's password and return the hashed result to the server. The server can similarly key-hash the sent random value using the client's password, as stored in a database on the server, and compare the results of the client's key-hash. If the two hashes are identical, then the client has proven knowledge of the shared secret and can be authenticated, without ever transmitting the shared secret. Mutual authentication can be performed in a similar manner, except that the server computing device now seeks to be authenticated by proving its knowledge of another shared secret.

Thus, paragraph [0044] only discloses hashing the shared secret. Paragraph [0044] does not disclose hashing both the first (e.g. tunnel) encryption key, second (e.g. authentication) encryption key.

Similarly, paragraph [0079] discloses that a challenge is sent, the response is the result of a one-way hash of the challenge and a shared secret (e.g. password). The challenger calculates an expected response and verifies the response to the challenge matches the calculated response. Paragraph [0079] like [0044] only hashes using the shared secret, not with both the first (e.g. tunnel) and second (e.g. authentication) keys.

New claim 28 further recites invalidating a secure credential for the second party responsive to a failure to establish the tunnel, authenticate and/or verifying the first and second keys. Invalidating a secure credential as used herein implies that the client must re-establish the secure credential by an out-of-band mechanism. By contrast, Funk & Palekar only deny access for one of these failures.

CONCLUSION

Reconsideration of the application is requested for the reasons set forth above. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: 8-20-2007

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009